Joshua H. Watson (CSBN 238058)
jwatson@justice4you.com
Gina M. Bowden (CSBN 252815)
gbowden@justice4you.com
CLAYEO C. ARNOLD, APC
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

John A. Yanchunis (Pro Hac Vice Admission Anticipated)
jyanchunis@forthepeople.com
Marcio W. Valladares (Pro Hac Vice Admission Anticipated)
mvalladares@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602-3644
Tel: (813) 223-5505
Fax: (813) 222-4733

Attorneys for Plaintiffs
Terry Myers, Sr., Charles O'Neal and those similarly situated

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

TERRY MYERS, SR., CHARLES O'NEAL, and those similarly situated, Plaintiffs, v. EQUIFAX INC., and DOES 1 through 50, inclusive, Defendants.	Case No.: CLASS ACTION COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF DEMAND FOR JURY TRIAL

Come now Plaintiffs TERRY MYERS, SR. and CHARLES O'NEAL, who on their own behalves and on behalf of all those similarly situated allege and complain by and through counsel as follows on information and belief, and who prays for relief from the court:

SUMMARY OF THE CASE

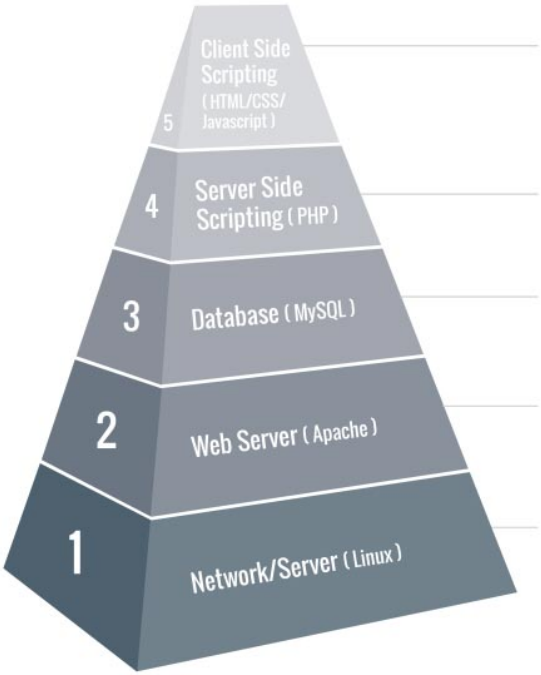
1. On or about July 29, 2017, Defendant EQUIFAX INC, DOES 1 to 50, and each of them (hereafter referred to collectively and individually as "Defendants") became aware of a data breach incident in which the personal data of some 143 Million people in the United States was improperly accessed and copied by persons outside the EQUIFAX INC. enterprise, hereafter referred to as the "subject data breach." EQUIFAX INC. admitted that the subject data breach occurred in or about mid-May of 2017 and July of 2017, though for the purposes of this Complaint, it is alleged that the data breach occurred during a broader period of time spanning the first half of 2017 up until the date of disclosure.

2. Defendants disclosed the subject data breach on or about September 8, 2017.

3. In the subject data breach, an unauthorized person, group, or entity outside the EQUIFAX INC. enterprise took sensitive personal information of consumers from Defendants by intruding into Defendants' computer system. The intrusion was accomplished by exploiting a website application operated by and/or on behalf of Defendants. That such a large breach of so much especially sensitive information took place in this manner demonstrates substantial negligence on the part of Defendants since web applications are known to require substantial security measures since they are accessible to the entire internet. Web applications operate as a "stack" of technologies and programs which interface with one another in order to produce what appears to be a singular application on the web. The stack includes (1) server and network hardware, (2) web server software; (3) database server software; (4) server-side scripting to control the behavior of the application on the computer hosting the application; (5) client-side scripting to control the behavior of the application on the computer displaying the application in a web browser or similar interface. Each layer of the stack includes various security strengths and weaknesses. Each layer of the stack operates with its own computer language/system, and communicates with the other layers of the stack. For instance, text typed into a web form on the

client-side scripting level is submitted to the server-side script, which interacts with both the server-side database and the web server software to alter data on the server's storage (e.g. hard drive array). A competently designed web application controls the flow of information between the levels of the stack to prevent improper commands from being executed in a harmful way, whether by accident or by persons with malicious intent. The graphic below is a fair representation of the stack for one type of common web application using "LAMP" architecture:

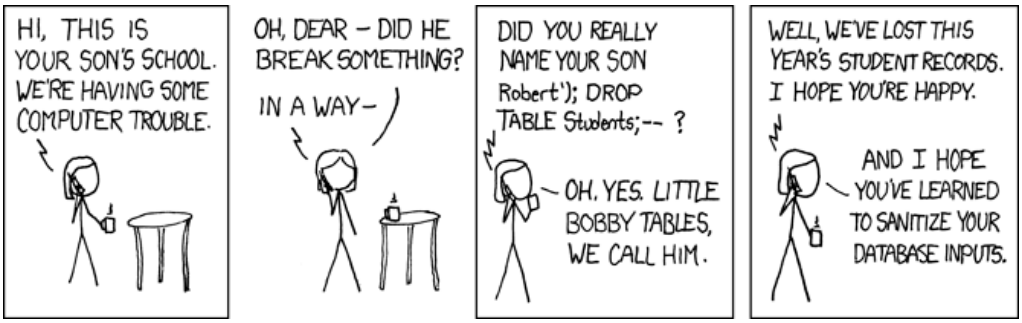
Fig. 1: LAMP Stacks



(Source: http://courses.haigarmen.com)

4. Ordinary due care in designing web applications requires implementation of security at each level of the stack. For instance, server-side scripts (level 4) should examine incoming text submitted by users on level 5 (web browser) to ensure it does not contain code that could damage the database (level 3), and neutralize such language if it appears. For instance, malicious users of a web application may add semicolons to their text in unprotected form fields (level 5) in order to send commands to the database (level 3) via the scripting language (level 4). Hence a classic comic strip circulated in programming circles about a student's name destroying his school's computer system:

Fig. 2. Comic Strip Reflecting Common Knowledge of Stack Security Concerns Among Programmers.



(Source: https://www.idtech.com/blog/part-ii-top-10-programmer-jokes-explained-for-the-rest-of-us/)

5. Common commands and techniques exist to prevent harm from such security issues, but developing a reasonably secure web application requires applying the appropriate measures at each level in a manner appropriate for the needs of the particular application.

6. If a web application involves use of sensitive information, due care requires that the stack be rigorously designed and configured with respect to preventing the flow of inappropriate commands or information. Examples of such due care include among other things: (1) including intrusion-detection measures to promptly alert of hacking if it occurs; (2) programming server-side scripts to prevent SQL-Injection attacks (such as the comic above); (3) removing any critical data-validation from the server-side script (where it can be edited by malicious users); (4) robust encryption; (5) strict data access control; and (6) avoiding negligent programming techniques, such as using the same names data containers across the stack (e.g. using "FirstName" in a web browser text box, which in turn feeds to a server-side variable named $FirstName, which in turn feeds to a database field FirstName; which taken as a whole allows a malicious user to map the database (level 3) simply by reading the code sent to his or her computer (level 5) by the web server (level 2).)

7. Rigorous design of the stack requires thoughtful systems design and enforcement of programming protocols within the team(s) of developers creating a web application. As a result, due care for web applications with access to highly sensitive information requires design of such

applications by hand-coding, without resort to quick-design tools that decrease development time, but at the expense of security (e.g. overuse of design programs like Dreamweaver or overuse of standardized well-known publically-accessible scripting frameworks in lieu of thoughtful stack design).

8. The nature and extent of the subject data breach in this Complaint illustrates that Defendants did not exercise due care in the design and maintenance of the subject web application. Had due care been used, any breach would have been promptly detected and stopped. Further, a breach of the magnitude at issue here would not have occurred because it would not have been possible to access the amount of highly confidential information as was accessed in the subject data breach.

9. Further, Defendants were generally negligent in their storage, maintenance, security, and inspection of their computer systems in such a manner that their negligence was a substantial factor in and proximate cause of the subject data breach.

10. Further, Defendants were generally negligent in their management of the subject data breach including but not limited to their technical response to the breach and the manner, timing, method, and content of their notice to affected persons regarding the breach.

11. The sensitive information obtained by unauthorized persons, groups, or entities in the subject data breach included but was not limited to names, contact information, date of birth, social security number, driver's license numbers, financial account information, information related to medical matters, information related to tax matters, and credit file information. This compromised data is collectively referred to as "Personal Identifying Information" or "PII."

12. In the subject data breach, Defendants negligently and unlawfully allowed unauthorized persons, groups, and/or entities to obtain PII about Plaintiffs and the class.

13. Defendants obtained PII about Plaintiffs and the class through various channels including but not limited to voluntary disclosure, disclosure mandated by third parties, disclosure obtained by Defendants through the operation of the credit industry, and disclosure obtained through the purchase and sale of PII by Defendants.

14. In this context, Defendants assumed statutory duties and duties of due care under

common law to safeguard the PII of Plaintiffs and the class.

15. Despite having knowledge of the subject data breach since at least July of 2017, Defendants waited months before disclosing it. During that time, Defendants held corporate meetings, purchased one or more identity theft consulting/monitoring/ protection firms, and operated their business in such fashion as to optimize their position with respect to the subject data breach – all without giving appropriate and timely notice to affected consumers so that consumers could protect their interests and identities. As a result, identity thieves had, during this time, unfettered access to the PII before Defendants even notified victims that their PII had been compromised.

16. Once Defendants did give notice, they coupled it with an illusory offer of protection. The offer included included one year of free identity theft monitoring in a company owned and operated by Defendants. However, it is well known and generally accepted as true that identity theft criminals hold data for more than one year – often for years – prior to using it. Therefore, one year of monitoring is not sufficient to protect Plaintiffs or the class. Contrary to being an offer of actual protection, Defendants' offer is more of a marketing scheme to turn a negative event into a profit opportunity by enrolling millions of Americans in their premium monitoring program for one year, and gaining the right and ability to directly market to them for other services and continued protection in future years at a price.

17. Further, in order to obtain such purported protection, Defendants require Plaintiffs and the class to suffer diminished rights regarding the subject data breach, including not limited to acceptance of an arbitration clause not otherwise applicable to Plaintiffs and the class.

18. This Class Action Complaint is filed on behalf of Plaintiffs and all persons, described more fully in the following sections, whose PII was compromised in the subject data breach. The class representative here has suffered actual harm, including but not limited to the need to pay for adequate and appropriate credit monitoring, incur the time and expense of investigating the potential for identity theft and the related need for account freezes, card and account replacements, and late fees for delayed payments. Class members have devoted and will continue to devote time and energy into recovering stolen funds (where possible), tracking and repairing

damage to their credit reports and reputations, and monitoring and protecting their accounts. Plaintiff and Class members are further damaged as their PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it for its commercial value, without Plaintiffs' or Class members' consent.

19. Plaintiffs and numerous class members suffered fraudulent transactions arising from the subject data breach. For instance:

a. Plaintiff MYERS utilizes a formal name for credit transactions, and a less formal name for other transactions. He utilizes a specific phone number for credit transactions. Following the subject data breach, MYERS suffered a sudden influx of spam, phishing attempts, and suspicious phone calls utilizing his formal name as contained in his credit file. In this same period, MYERS suffered a number of fraudulent financial transactions in his formal name. Prior to the subject data breach, he had not suffered substantially similar issues. There is no plausible alternative link between the sudden increase of fraudulent activity in his formal name other than the subject data breach.

b. Following the subject data breach, Plaintiff O'NEAL was informed that two of his bank cards had been compromised with fraudulent transactions. He was required to cancel the cards and obtain new ones due to actual events of identity-theft-related monetary losses consistent with use of his identity using information obtained in the subject data breach.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because, on information and belief, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants. Subject matter jurisdiction also arises under 28 U.S.C. § 1331 based on the claim asserted under the Federal Stored Communications Act, 18 U.S.C. § 2702. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District. Venue is also proper because the impact of the subject data breach was felt by the named plaintiffs in Sacramento County and San Joaquin County, which are both within this Court's venue.

PARTIES

22. Plaintiff TERRY MYERS, SR. (hereafter "MYERS") is a resident of San Joaquin County, California. His data was lost by Defendants in the subject data breach.

23. Plaintiff CHARLES O'NEAL (hereafter "O'NEAL") is a resident of Sacramento County, California. His data was lost by Defendants in the subject data breach.

24. Defendant EQUIFAX INC. is a publically traded Georgia corporation registered with the California Secretary of State, with its principal place of business and headquarters at 1550 Peachtree Street, N.W., Atlanta, Georgia.

25. The true names and capacities of Defendants sued herein as DOES 1 through 50, inclusive, are currently unknown to Plaintiff, who therefore sues such Defendants by such fictitious names. Each of the Defendants designated herein as a DOE is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of Court to amend this Complaint to reflect the true names and capacities of the Defendants designated herein as DOES when such identities become known.

26. Based upon information and belief, Plaintiff alleges that at all times mentioned herein, each and every Defendant and DOE was acting as an agent and/or employee and/or joint venture of each of the other Defendants and DOE, and at all times mentioned was acting within the course and scope of said agency and/or employment and/or joint venture with the full knowledge, permission, consent and ratification of each of the other Defendants and DOES. In of addition, each of the acts and/or omissions of each Defendant and DOE alleged herein were made known to, and ratified by, each of the other Defendants and DOES.

FACTUAL BACKGROUND

27. EQUIFAX INC describes itself as follows in its 2016 10k filing with the US SEC: "Equifax Inc. is a leading global provider of information solutions and human resources business

process outsourcing services for businesses, governments and consumers. We have a large and diversified group of clients, including financial institutions, corporations, governments and individuals. Our products and services are based on comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data. We use advanced statistical techniques and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for our clients. We help consumers understand, manage and protect their personal information and make more informed financial decisions. We also provide information, technology and services to support debt collections and recovery management. Additionally, we are a leading provider of payroll-related and human resource management business process outsourcing services in the United States of America, or U.S."

28. EQUIFAX, DOES 1 to 50, and each of them (hereafter, "Defendants") operate as a common enterprise with respect to the subject data breach.

29. In the course of such operations, Defendants obtain financial gain by, among other things, collecting and selling PII about Americans, including Plaintiffs and the class.

30. Some such PII is obtained by Defendants directly from consumers via direct communications and contract with consumers. Some such PII is obtained by Defendants via authorization by consumers via third party in which consumers and Defendants enter into an agreement concerning the use of consumers' PII. Some such PII is obtained by Defendants in other circumstances giving rise to statutory and common law duties by Defendants to Plaintiffs and the class.

31. Defendants did not notify timely Plaintiffs and the class that their PII had been involved in the subject data breach.

32. Plaintiffs have at no point provided any binding release to Defendants with respect to any liability which may arise from the subject data breach.

33. Class members have at no point provided any binding release to Defendants with respect to any liability which may arise from the subject data breach.

34. The circumstances of the subject data breach with respect to disclosure of Plaintiff's PII is typical of a broader class of claimants whose PII was involved in the subject data breach.

35. The circumstances of the disclosure of the subject data breach with respect Plaintiff is typical of a broader class of claimants whose PII was involved in the subject data breach.

36. The number of claimants whose PII was involved in the subject data breach was of sufficient number as to justify resolving this matter as a class action, provided the other aspects of class action certification are met.

37. The types of information compromised in the subject data breach are highly valuable to identity thieves. Names, email addresses, telephone numbers, dates of birth, social security numbers, address histories, information relevant to medical matters, and credit file information for Plaintiffs and those similarly situated.

38. Identity thieves can use the PII obtained in the subject data breach to harm Plaintiffs and Class members through theft, fraudulent transactions, embarrassment, blackmail or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration. The PII off the class certainly includes information posing the risk of such harm due to the nature and purposes of Defendants' investigation and litigation efforts.

39. In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information

in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

40. Plaintiffs have incurred actual loss of their identities as evidenced in the pleadings above, and are incurring mitigation expenses, including but not limited to the cost of appropriate and rigorous ongoing identity theft detection service, as well as the time and expense of obtaining and reviewing their credit reports. Such investigation, given the recent nature of the disclosure of the data breach, is ongoing at the time of filing and will result in incurring further expenditures of time and money.

41. To put it into context the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298 dollars.

42. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, a Government Accountability Office study found that "stolen data may be held for up to a year or more before being used to commit identity theft." (*See* Report to Congressional Requesters, U.S. Government Accountability Office, 33 (June 2007), available at www.gao.gov/new.items/d07737.pdf.) In order to protect themselves, class members will need to remain vigilant against unauthorized data use for years and decades to come.

43. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII. Websites appear and disappear quickly, making it a very dynamic environment. (*See* Brian Hamrick, The dark web: A trip into the underbelly of the internet, WLWT News (Feb. 9, 2017 8:51 PM), http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the- internet/8698419.)

44. Once someone buys PII, it is then used to gain access to different areas of the victim's

digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

45. The sale of PII occurs in an active criminal market. The risk of crime to which identity theft victims such as Plaintiff and Class members are exposed is captured by the logo of a dark web sales site that features a satirical gun wielding Ronald McDonald and the moto, "i'm swipin' it:"

(*See* https://krebsonsecurity.com/2014/06/peek-inside-a-professional-carding-shop/)

CLASS ACTION ALLEGATIONS

44. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following:

A. The overall class, which includes each subclass below: All persons (including natural and legal persons) whose PPI was disclosed in the subject breach due to his/her/its PII being included in the materials that were taken from Defendants

B. The California Subclass: This class includes class members who also reside in California or otherwise are the beneficiaries of California law governing PII or data security.

45. Collectively, all of the classes will be referred to herein as the "Class," except where otherwise noted in order to differentiate them.

46. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and

employees.

47. Numerosity: The members of each Class are so numerous that joinder of all members of any Class would be impracticable. The names and addresses of Class members are identifiable through documents maintained by Defendants.

48. Commonality and Predominance: This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

A. For All Classes:

i. Whether Defendants represented to the Class assumed a duty to safeguard Class members' PII;

ii. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iii. Whether Defendants breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iv. Whether Class members' PII was accessed, compromised, or stolen in the subject data breach;

vii. Whether Defendants knew about the subject data breach before it was announced and failed to timely notify affected persons of the breach;

viii. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

ix. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

B. As to the California Subclass:

i. Whether subclass is entitled to relief under California law.

49. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of their respective classes. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the

numerous common questions that dominate this action.

50. Typicality: Plaintiff's claims are typical of the claims of the other members of the class because, among other things, Plaintiff and the other class members were injured through the substantially uniform misconduct by Defendants. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

51. Adequacy of Representation: Plaintiff is an adequate representative of the classes because Plaintiff's interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

52. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other members of the class are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

53. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

54. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class members' PII was accessed, compromised, or stolen in the subject breach;

b. Whether (and when) Defendants knew about any or all of the subject breach before it was announced to the public and failed to timely notify the public of the subject breach;

e. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

f. Whether Defendants breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

g. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, et seq.;

h. Whether it was reasonable for Plaintiff and Class members to expect that Defendants would secure and protect the PII and financial information of Plaintiffs and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services (where applicable);

j. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

k. Whether Plaintiffs and the other class members are consumers within the meaning of Cal. Civ. Code §1761(d);

l. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

m. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII or financial information secure and prevent the loss or misuse of that information;

First Claim for Relief

Violation of California's Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code § 17200, et seq.)

By All Plaintiffs and California Subclass Against All Defendants

55. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained above as though fully stated herein.

56. By reason of the conduct alleged herein, Defendants engaged in unlawful, unfair, and deceptive practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

57. Defendants stored the PII of Plaintiff and members of their respective classes in Defendants' electronic files, as reflected by the nature and circumstances of the subject data breach.

58. Reasonable security measures would have prevented such a data breach as the one at issue here, including but not limited to securing the web application stack.

59. Defendants' method of storing, accessing, transferring, controlling, monitoring, securing, and managing use of the subject PII was at all relevant times a business practice within the meaning of Cal. Civil Code 17200.

60. Plaintiffs and Class members were entitled to, and did, assume Defendants would take appropriate measures to keep their PII safe. Defendants did not disclose at any time that Plaintiffs' PII was vulnerable to hackers because Defendants data security and use policies and practices were inadequate or outdated.

61. Defendants knew or should have known they did not employ reasonable measures that would have kept Plaintiff's and the other Class members' PII secure and prevented the loss or misuse of Plaintiffs' and the other class members' PII.

62. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Cal. Civ. Code § 1798.80 et seq.; 15 USC § 6801; 15 U.S.C. § 45.

63. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Defendants' failure to secure Plaintiff's and the other Class members' PII

contained in their servers or databases.

64. As a result of Defendant's violations of the UCL, Plaintiff and the other Class members are entitled to equitable relief as provided for by law, including but not limited to injunctive relief, disgorgement, and restitution.

Second Claim for Relief

Violation of California's Customer Records Act

By All Plaintiffs and California Subclass Against All Defendants

65. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained above as though fully stated herein.

66. Defendants, and each of them, were at all relevant times parties subject to the California Customer Records Act (herein "CPA"), including but not limited to the CPA's requirements regarding securing data as set forth at Cal. Civil Code §§ 1798.80, et seq, including but not limited to § 1798.81.5 (regarding security procedures and practices) and § 1798.82 (regarding disclosure requirements). Plaintiff and the class note § 1798.84 of the CPA, which provides for a private right of action for affected persons.

67. All California Class members, including Plaintiffs, were at all relevant times persons whose data with Defendants was subject to the protections of CPA. Notwithstanding the statute's title, CPA protects all residents of California, not just California-based customers. See, e.g., Civ. Code, § 1798.81.5 ["A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."]; Civ. Code § 1798.82 ["A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California.."]

68. As alleged herein, Defendants breached their duties to Plaintiff and Class members with respect to safeguarding their PII, and such breaches violated CPA obligations, including those

arising under Civ. Code, § 1798.81.5.

69. As alleged herein, Defendants breached their duties to Plaintiff and California Subclass members with respect to timely disclosure of the data breach. The months of delay between Defendants' notice of the breach and the date of their disclosure subjected Plaintiffs and Class members to increased risk of identity theft and other harm associated with the breach.

70. As a direct and proximate result of Defendants' violations of CPA, Plaintiff and Class members suffered injury and attendant damages, and as a result are entitled to recover damages, costs, and attorney fees per statute.

Third Claim for Relief

Negligence

By All Plaintiffs and Class Members Against All Defendants

71. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained above as though fully stated herein.

72. Defendants, and each of them, owed a duty of care to Plaintiff and Class members with respect to the collection, storage, security, use, and disclosure of their PII. This duty of care included taking reasonable steps to keep the PII safe from inadvertent or deliberate disclosure or removal, including by hacking or other malicious intrusion, and a duty to promptly inform any affected person whose PII was taken from Defendants.

73. Defendants, and each them assumed such duties when they accepted receipt of PII regarding Plaintiffs and Class members and used such information substantially for their own benefit.

74. The duty of Defendants is also established by statute, including but not limited to the statutes cited herein: Cal. Civ. Code § 1798.80 et seq.; 15 USC § 6801; and 15 U.S.C. § 45.

75. Defendants, and each of them, breached their duty to Plaintiff and Class members as alleged herein, including but not limited to failing to store and secure the PII with reasonable care, failing to appropriately prevent the removal/disclosure of the PII, failing to appropriately detect the removal/disclosure of the PII, and failing to appropriately and timely notify Plaintiff and Class members of the removal/disclosure of the PII.

76. As a direct and proximate result of the breach of care by Defendants, and each of them, Plaintiff and Class members suffered injury and attendant damages, and as a result are entitled to recover damages and costs by law.

Fourth Claim for Relief

Negligence Per Se

By All Plaintiffs and Class Members Against All Defendants

77. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained above as though fully stated herein.

78. The negligence of Defendants is presumed by common law principles of Negligence Per Se and as those are codified at Cal. Civil Code 669.

79. Defendants violated statutes, ordinances, and regulations of a public entity in acting as alleged herein including but not limited to Cal. Civ. Code § 1798.80 et seq.; 15 USC § 6801; and 15 U.S.C. § 45.

80. The violation of these statutes directly and proximately caused injury to Plaintiffs and Class members as alleged herein since if Defendants had complied with the statutes the removal/disclosure of PII would never have occurred in the first place. In the alternative, had it occurred, Planitiffs and Class members would have received prompt notice and the ability to begin mitigating damages.

81. Plaintiff and Class members were of the category of persons to be protected by these statutes.

82. As a direct and proximate result of the Defendants' violations of statute them, Plaintiff and Class members suffered injury and attendant damages, and as a result are entitled to recover damages and costs by law.

Fifth Claim for Relief

Declaratory Relief

By All Plaintiffs and Class Members Against All Defendants

77. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained above as though fully stated herein.

78. In connection with the active case and controversy between Plaintiffs and Defendants, Plaintiffs seek declaratory relief pursuant to 28 U.S.C. § 2201, declaring that:

a. That Defendants owe a duty of care to Plaintiffs and Class members to take reasonable steps to secure their data from unauthorized access while that data is within Defendants' custody;

b. That Defendants are parties subject to the obligations of Cal. Civ. Code § 1798.80 et seq.; 15 USC § 6801; and 15 U.S.C. § 45;

c. That Claimant Class Members' right to fair business practices includes the right, pursuant to Cal. Bus. & Prof Code 17200, to have Defendants use modern and secure methodologies to protect their PII possessed by Defendants;

d. That Defendants' data security policies as related to the subject data breach are below the level required to satisfy the legal rights of Plaintiff and Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests that this Court enter an Order:

(a) Certifying each proposed class and appointing Plaintiffs as Class Representatives;

(b) Finding that Defendants' conduct was negligent, unfair, and unlawful as alleged herein;

(c) Enjoining Defendants from engaging in further negligent, unfair, and unlawful business practices alleged herein;

(d) Awarding Plaintiffs and the Class members actual, compensatory, and consequential damages;

(e) Awarding Plaintiffs and the Class members statutory damages and penalties, as allowed by law;

(f) Awarding Plaintiffs and the Class members restitution and disgorgement;

(g) Requiring Defendants to provide appropriate credit monitoring services to Plaintiff and the other class members;

(h) Awarding Plaintiff and the Class members pre-judgment and post-judgment

interest;

(i) Awarding Plaintiff and the Class members reasonable attorneys' fees costs and expenses, and;

(j) Granting such other relief as the Court deems just and proper.

For the purposes of due process and default judgment regarding claims not characterized as personal injury, Plaintiff and Class members set forth a prayer of not more than $75,000,000,000 (Seventy Five Billion US Dollars) understanding this amount be arrived at purely for reservation of rights for these purposes and is subject to change, including increase, during litigation of this matter.

Dated: September 8, 2017

CLAYEO C. ARNOLD, APC

By: /s/ Joshua H. Watson
Joshua H. Watson

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 8, 2017

CLAYEO C. ARNOLD, APC

By: /s/ Joshua H. Watson
Joshua H. Watson